

CLAIMS

1 1. A network processor, comprising:

2 an authentication buffer to store authentication data including at least one of ciphered-
3 network-packet data subject to authentication, network packet data subject only to
4 authentication, and network packet data subject to ciphering and authentication, wherein the
5 authentication buffer includes a circular first-in-first-out (FIFO) arrangement; and

6 at least one authentication core coupled to the authentication buffer to authenticate the
7 authentication data from the authentication buffer.

8
9 2. The network processor of Claim 1, wherein the circular FIFO arrangement includes a
10 moveable start of data pointer and a moveable end of data pointer.

11
12 3. The network processor of Claim 1, wherein the network processor further includes at
13 least one cipher core adapted to operate with a cipher algorithm and the at least one
14 authentication core is adapted to operate with an authentication algorithm, and a size of the
15 authentication buffer is selected in accordance with a data block size associated with the cipher
16 algorithm and a data block size associated with the authentication algorithm.

17
18 4. The network processor of Claim 1, wherein the authentication core is adapted to
19 authenticate the authentication data from the authentication buffer as blocks of authentication
20 data.

21
22 5. A network, comprising:

23 a network processor having:

24 an authentication buffer to store authentication data including at least one
25 of ciphered-network-packet data subject to authentication, network packet data
26 subject only to authentication, and network packet data subject to ciphering and
27 authentication, wherein the authentication buffer includes a circular first-in-first-
28 out (FIFO) arrangement; and

1 at least one authentication core coupled to the authentication buffer to
2 authenticate the authentication data from the authentication buffer.

3
4 6. The network of Claim 5, wherein the circular FIFO arrangement includes a moveable
5 start of data pointer and a moveable end of data pointer

6
7 7. The network of Claim 5, wherein the network processor further includes at least one
8 cipher core adapted to operate with a cipher algorithm and the at least one authentication core is
9 adapted to operate with an authentication algorithm, and a size of the authentication buffer is
10 selected in accordance with a data block size associated with the cipher algorithm and a data
11 block size associated with the authentication algorithm.

12
13 8. The network of Claim 5, wherein the authentication core is adapted to authenticate the
14 authentication data from the authentication buffer as blocks of authentication data.

15
16 9. A method of authenticating network packet data, comprising: ~
17 moving to an authentication buffer authentication data including at least one of
18 ciphered-network-packet data subject to authentication, network packet data subject only to
19 authentication, and network packet data subject to ciphering and authentication, wherein the
20 authentication buffer includes a circular first-in-first-out (FIFO) arrangement; and
21 moving to an authentication core a block of data from the authentication buffer.

22
23 10. The method of Claim 9, wherein the moving to an authentication buffer authentication
24 data comprises selecting the authentication buffer from among a plurality of authentication
25 buffers.

26
27 11. The method of Claim 9, further including:
28 setting a start of data pointer and an end of data pointer to respective initial locations;
29 setting the end of data pointer in accordance with the moving the authentication data to
30 the authentication buffer; and

1
2 setting the start of data pointer in accordance with the moving to the authentication core
3 the block of data from the authentication buffer.

4
5 12. The method of Claim 9, wherein the authentication buffer includes a circular first-in-
6 first-out (FIFO) arrangement.

7
8 13. The method of Claim 9, further including:
9 providing a cipher core adapted to operate with a cipher algorithm;
10 providing the authentication core adapted to operate with an authentication algorithm,
11 and
12 sizing the authentication buffer in accordance with a data block size associated with the
13 cipher algorithm and a data block size associated with the authentication algorithm.

14
15 14. A computer program medium having computer readable code thereon to authenticate
16 network packet data, the medium comprising:
17 instructions for moving to an authentication buffer authentication data including at least
18 one of ciphered-network-packet data subject to authentication, network packet data subject only
19 to authentication, and network packet data subject to ciphering and authentication, wherein the
20 authentication buffer includes a circular first-in-first-out (FIFO) arrangement; and
21 instructions for moving to an authentication core a block of data from the authentication
22 buffer.

23
24 15. The method of Claim 14, wherein the instructions for moving to an authentication
25 buffer authentication data comprises instructions for selecting the authentication buffer from
26 among a plurality of authentication buffers.

27
28 16. The method of Claim 14, further including:
29 instructions for setting a start of data pointer and an end of data pointer to respective
30 initial locations;

1 instructions for setting the end of data pointer in accordance with the moving the
2 authentication data to the authentication buffer; and
3 instructions for setting the start of data pointer in accordance with the instructions for
4 moving to the authentication core the block of data from the authentication buffer.
5

6 17. The computer program medium of Claim 14, wherein the authentication buffer includes
7 a circular first-in-first-out (FIFO) arrangement.
8

9 18. The computer program medium of Claim 14, further including:

10 instructions for providing a cipher core adapted to operate with a cipher algorithm;

11 instructions for providing the authentication core adapted to operate with an
12 authentication algorithm, and

13 instructions for sizing the authentication buffer in accordance with a data block size
14 associated with the cipher algorithm and a data block size associated with the authentication
15 algorithm.